UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,026	10/10/2000	Marco Martins	YOR9-2000-0165	2558

21254 7590 09/30/2004

MCGINN & GIBB, PLLC
8321 OLD COURTHOUSE ROAD
SUITE 200
VIENNA, VA 22182-3817

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/685,026	**Applicant(s)** MARTINS ET AL.	
	Examiner Brandon Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 July 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending in this office action.

2. Applicant's arguments filed July 1, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1, 3-7, 9, 13, 24, 25, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S. Patent No. 6,466,671).

Regarding claims 1 and 27, Leppek teaches [a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform] a method for preventing counterfeiting and cloning of smart cards, comprising: providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined number of readings (abstract and col. 4, lines 8-66), wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (col. 4, lines 33-38, the key supplies the proper sequence).

Leppek does not teach the device is a smart card.

Maillard et al. teaches the device is a smart card (abstract).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to implement the teachings of Leppek onto a smart card, as taught by Maillard et al. It would have been obvious to one of ordinary skill in the art to implement the teachings of Leppek onto a smart card, as taught by Maillard et al., because smart cards are small, easy to use mediums for encryption; to provide a method which prevents a footprint or playback attack from being performed by an intruder would help spread the acceptance of smart cards used in technology (see col. 2, lines 25-38 of Leppek).

Regarding claim 3, the combination of Leppek in view of Maillard et al. teaches wherein an entire process of said method is performable off-line (the Examiner takes Official Notice that in smart card technology, comprising a reader, the transfer of information from smart card to reader is performed off-line, meaning no network connection is established for obtaining key information or other information needed to authenticate the device).

Regarding claim 4, the combination of Leppek in view of Maillard et al. teaches wherein said smart card carries thereon predetermined N channels as C1, C2, ..., CN, where N is an integer (see fig. 2, ref. num 100 of Leppek), wherein each channel Ci, with i equal to 1, 2, ..., N, carries a pair of numbers (hi, li), and wherein hi is the i^{th} high number and li is the i^{th} low number (see fig. 2, ref. num 110-1 through 110-N of Leppek).

Regarding claim 5, the combination of Leppek in view of Maillard et al. teaches further comprising:

- Using public key cryptography with associated encoding and decoding functions Vi and Vi-^{1} in each channel i,
- Wherein each function Vi-' is known publicly, and Vi is known only to a predetermined party representing an owner of the smart card (see page 6, lines 1-5 of applicants disclosure, applicant submits this information is well known as taught by Menezes et al.).

Regarding claim 6, the combination of Leppek in view of Maillard et al. teaches:

- Wherein for each i in 1, 2, ..., N, the pair (hi, li) is such that hi = Vi(li), or hi = Vi(K(li)), where K represents a publicly-known cryptographic hash function, and
- Wherein each li contains a plurality of symbols for redundancy (see page 6, lines 6-8 of applicants disclosure, applicant submits this information is well known as taught by Menezes et al.).

Regarding claim 7, the combination of Leppek in view of Maillard et al. teaches further comprising processing, using an invertible function f which is made public, such that the low numbers in said smart card satisfy $l(i+j) = f^j(li)$, where f^j represents the j^{th} iteration of the function f (see col. 5, lines 19-52 of Leppek).

Regarding claim 9, the combination of Leppek in view of Maillard et al. teaches wherein a reader obtains a content of only two of said channels (see col. 4, lines 33-42 of Leppek, the number does not specifically state two, but is any number less than the total number of keys contained in the smart card).

Regarding claim 13, the combination of Leppek in view of Maillard et al. teaches wherein said cryptographic structure is changed periodically (see col. 1, lines 41-47 of Maillard et al.).

Regarding claim 24, Leppek teaches a method of preventing counterfeiting of a smart card, comprising:

- Providing a smart card such that none of confidential information and a cryptographic key for authorizing the smart card, is carried on the smart card (col. 4, lines 7-17);
- Reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique (col. 4, lines 33-42).

Leppek does not specifically teach the device is a smart card or that a card reader performs the reading.

Maillard et al. teaches the device is a smart card (fig. 2, ref. num 3020) and a card reader performs the reading (fig. 2, ref. num 2020).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the device being a smart card and the reading is a card reader, as taught by Maillard et al., with the method of Leppek. It would have been obvious to combine the device being a smart card and the reading is a card reader, as taught by Maillard et al., with the method of Leppek because smart cards are small, easy to use mediums for encryption and a card reader would be required to read the data contained on the small smart card.

Regarding claim 25, the combination of Leppek in view of Maillard et al. teaches wherein a transaction performed under said method comprises substantially an off-line transaction (the Examiner takes Official Notice that in smart card technology, comprising a reader, the transfer of information from smart card to reader is performed off-line, meaning no network connection is established for obtaining key information or other information needed to authenticate the device).

Claims 2, 10-12, 14, 23, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S. Patent No. 6,466,671), and further in view of Perlman et al. (U.S. Patent No. 5,261,002).

Regarding claim 2, the combination of Leppek in view of Maillard et al. teaches providing a reader for reading said smart card (fig. 2, ref. num 2020 of Maillard et al.). However, the combination of Leppek in view of Maillard et al. does not teach further comprising including a database holding information related to unauthorized smart cards, said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network.

Perlman et al. teaches further comprising including a database holding information related to unauthorized smart cards (col. 6, lines 37-39), said reader being on-line, such that said reader is operatively connected to a network, only when said database of said reader is being updated by said network (col. 3, lines 38-40 and fig. 1, ref. num 24-30, the concept of the invention in Perlman et al., when applied to Leppek and Maillard et al., shows a receiver (reader) of a request from a potential intruder (smart card) performing the steps necessary to check a blacklist of already expired or invalid intruders (smart cards)).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine including a database of unauthorized smart cards and periodically going online with the reader to obtain a newer list, as taught by Perlman et al., with the method of Leppek/Maillard et al. It would have been obvious to combine including a database of unauthorized smart cards and periodically going online with the reader to obtain a newer list, as taught by Perlman et al., with the method of Leppek/Maillard et al. because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known, without performing the update constantly – tying up a lot of resources.

Regarding claim 10, the combination of Leppek in view of Maillard et al. teaches all the limitations of claim 1 above. However, the combination of Leppek/Maillard et al. does not teach further comprising periodically communicating, by a reader of said smart card, with a database where a predetermined characteristic of the card is checked.

Perlman et al. teaches further comprising periodically communicating, by a reader of said smart card, with a database where a predetermined characteristic of the card is checked (col. 3, lines 38-40 and fig. 1, ref. num 16-18).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine periodically communicating with a database where a predetermined characteristic of the card is checked, as taught by Perlman et al., with the method of Leppek/Maillard et al. It would have been obvious to combine periodically communicating with a database, as taught by Perlman et al., with the method of Leppek/Maillard et al. because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known, without performing the update constantly – tying up a lot of resources.

Regarding claim 11, the combination of Leppek in view of Maillard et al. and further in view of Perlman et al. teaches wherein the predetermined characteristic comprises whether a smart card has delivered more than a predetermined amount of money to a user of the smart card (see col. 7, lines 21-23 of Perlman et al., although Perlman discloses the predetermined condition to be a preset time limit, other reasons for refusing the smart card exist, dependent on the use of the card. In this case it is certificates, so the time limit is a predetermined condition. In the case of a money card, a limit spent or received would be an obvious threshold.).

Regarding claim 12, the combination of Leppek in view of Maillard et al. and further in view of Perlman et al. teaches wherein if a card is detected as delivering too much money, the database communicates a corresponding number I1 to all readers in a network, so that smart cards carrying said corresponding number are declined (see col. 7, lines 14-26 of Perlman et al.).

Regarding claim 14, the combination of Leppek in view of Maillard et al. teaches all the limitations of claim 1, above. However, the combination of Leppek in view of

Maillard et al. does not teach wherein said smartcard is invalidated after a predetermined time of usage.

Perlman et al. teaches wherein said smartcard is invalidated after a predetermined time of usage (fig. 2, ref. num 42).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine invalidating the smart card after a predetermined time of usage, as taught by Perlman et al., with the method of Leppek/Maillard et al. It would have been obvious to combine invalidating the smart card after a predetermined time of usage, as taught by Perlman et al., with the method of Leppek/Maillard et al. because the time limit threshold provides more security by allowing only a certain time of use. After the time limit has expired, it would be safe to say that the user did not want to use the card anymore, or if the user does want to use the card, the user can renew his/her time for the card.

Regarding claim 23, the combination of Leppek in view of Maillard et al. teaches that the device is a smart card and there exists a reader for reading the smart card (see fig. 2, ref. num 2020 and 3020). However, the combination of Leppek in view of Maillard et al. does not teach further comprising: performing a final validation of the smart card by at least one of: contacting a central database if an entire transaction is made on-line with no penalty; and checking with a local database in a reader, said local database being refreshed periodically by contact between said local database and said central database.

Perlman et al. teaches further comprising:

- Performing a final validation of the smart card by at least one of: contacting a central database if an entire transaction is made on-line with no penalty; and checking with a local database in a reader (col. 6, lines 37-39),
  - Said local database being refreshed periodically by contact between said local database and said central database (col. 3, lines 38-40 and fig. 1, ref. num 24-30).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the reader including a database for linking to a network for periodic updates, as taught by Perlman et al., with the system of Leppek/Maillard et al. It would have been obvious to combine the reader including a database that is periodically updated, as taught by Perlman et al., with the system of Leppek/Maillard et al. because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known, without performing the update constantly – tying up a lot of resources.

Regarding claim 26, Leppek teaches a system for preventing cloning of a smart card, comprising:

- A smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card (col. 4, lines 7-17); and
- Wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof (col. 4, lines 33-38, the key supplies the proper sequence).

Leppek does not teach the device is a smart card or a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards.

Maillard et al. teaches the device is a smart card (fig. 2, ref. num 3020) and a reader for reading the smart card (fig. 2, ref. num 2020).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the device being a smart card and the reading is a card reader, as taught by Maillard et al., with the method of Leppek. It would have been obvious to combine the device being a smart card and the reading is a card reader, as taught by Maillard et al., with the method of Leppek because smart cards are small, easy to use mediums for encryption and a card reader would be required to read the data contained on the small smart card.

The combination of Leppek in view of Maillard et al. still does not teach reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards.

Perlman et al. teaches reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards (col. 6, lines 37-39 and col. 3, lines 38-40 and fig. 1, ref. num 24-30).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the reader including a database for linking to a network for periodic updates of unauthorized smart cards, as taught by Perlman et al., with the system of Leppek/Maillard et al. It would have been obvious to combine the reader including a blacklist database that is periodically updated, as taught by Perlman et al., with the system of Leppek/Maillard et al. because the off-line version of the blacklist provides a listing of all users who are intruders; the periodic updating allows a newer list of intruders to be known, without performing the update constantly – tying up a lot of resources.

Claims 8, 15-18, and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S Patent No. 6,466,671), and further in view of Schneier, "Applied Cryptography:

Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter referred to as Schneier).

Regarding claim 8, the combination of Leppek in view of Maillard et al. teaches all the limitation of claims 1 and 4-6, above. However, the combination of Leppek in view of Maillard et al. does not teach wherein a reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of distinct numbers with a < b between 1 and N, wherein before processing the smart card, the reader obtains the pair (ha, la) and hb; using the public keys Va-^{1} and Vb-^{1}, checking by the reader whether the pairs (ha, la) and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a same legitimate card.

Schneier teaches

- Wherein a reader includes a random number generator, which, when a card is read, chooses a pair (a, b) of distinct numbers with a < b between 1 and N, wherein before processing the smart card, the reader obtains the pair (ha, la) and hb (a step of an RSA algorithm, choose two prime numbers, page 467);
- Using the public keys Va-^{1} and Vb-^{1}, checking by the reader whether the pairs (ha, la) and (hb, lb) are compatible, and, consequently, that the numbers ha, la, and hb belong to a same legitimate card (a step of an RSA algorithm, page 467).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a random number in the reader, choose a pair of distinct numbers, and using the public keys to check the compatibility of the smart card, as taught by Schneier, to the method of Leppek/Maillard et al. It would have been obvious to combine generating a random number in the reader, choose a pair of distinct numbers, and using the public keys to check the compatibility of the smart card, as taught by Schneier, to the method of Leppek/Maillard et al. because these limitations verify a proper smart card based on the key checking, known as a digital signature.

Regarding claim 15, the combination of Leppek as modified by Maillard et al./Schneier teaches wherein said pairs (hi, li) to be contained on the smart card are generated by:

- Choosing a prefix of l1 once for all transactions, or changed whenever needed, wherein said prefix is publicly known (a step of an RSA algorithm, see page 467 of Schneier); and
- Providing a sequence, such that the sequence is generated so that a same number is not chosen twice, and so that corresponding other li's are not chosen as new l1s (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 16, the combination of Leppek as modified by Maillard et al./Schneier teaches further comprising:

- Concatenating the prefix and the sequence to form I1 (a step of an RSA algorithm, forming the product of two primes, see page 467 of Schneier); and
- Choosing a function f which is invertible and is publicly known, to construct I2 = f(I1), I3 f(I2), and so forth (a step of an RSA algorithm, use Euclidean algorithm on two primes, see page 467 of Schneier).

Regarding claim 17, the combination of Leppek as modified by Maillard et al./Schneier teaches wherein the function f is chosen to be the identity map, in which case I1 = I2 = I3 = ... =IN (a step of an RSA algorithm, where the message is encrypted in blocks, where the same encryption method is used for each block, see page 467 of Schneier).

Regarding claim 18, the combination of Leppek as modified by Maillard et al./Schneier teaches choosing, for a number N, N public key-private key pairs, such that a first private key V1 is for computing h1 = V1 (I1), a second private key V2 is for computing h2 = V2(I2), and so on (a step of an RSA algorithm, where the message is encrypted in blocks, see page 467 of Schneier).

Regarding claim 20, the combination of Leppek in view of Maillard et al. teaches all the limitations of claim 1, above. However, the combination of Leppek in view of Maillard et al. does not teach wherein, when the smart card is read by a reader, a random generator is prompted which provides two integer numbers, a and b, which are not between 1 and N, with a < b.

Schneier teaches wherein, when the smart card is read by a reader, a random generator is prompted which provides two integer numbers, a and b, which are not between 1 and N, with a < b (a step of an RSA algorithm, see page 467 of Schneier).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a random number in the reader and choose a pair of distinct numbers, as taught by Schneier, to the method of Leppek/Maillard et al. It would have been obvious to combine generating a random number in the reader and choose a pair of distinct numbers, as taught by Schneier, to the method of Leppek/Maillard et al. because these limitations select a public key of the reader for use in a public key algorithm.

Regarding claim 21, the combination of Leppek as modified by Maillard et al./Schneier teaches wherein said numbers a, b are transmitted to the smart card which delivers two high numbers ha, hb, and a low number la in a channel a, and wherein the pair (a, b), together with a function f in a memory in the reader, are used to compute the low number $lb=f^{(b-a)}(la)$, said memory in said reader delivering public keys Va^{-1} and Vb^{-1} (a step of an RSA algorithm, see page 467 of Schneier).

Regarding claim 22, the combination of Leppek as modified by Maillard et al./Schneier teaches wherein the public keys are used by a comparator together with the pairs (ha, la) and (hb, lb), to verify that the pairs are compatible with the corresponding keys, and that the pairs are from a same legitimate card (a step of an RSA algorithm, see page 467 of Schneier).

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S. Patent No. 6,466,671) and in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," Second Edition, pps. 466-474 (hereinafter referred to as Schneier), and further in view of Perlman et al. (U.S. Patent No. 5,261,002).

Regarding claim 19, the combination of Leppek as modified by Maillard et al./Schneier teaches further comprising: verifying whether the smart card is authentic (digital signature of an RSA algorithm, see page 473 of Schneier).

The combination of Leppek as modified by Maillard et al./Schneier does not teach checking whether the smart card is not in a list of cards to be refused.

Perlman et al. teaches checking whether the smart card is not in a list of cards to be refused (col. 6, lines 37-39).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine including a database of unauthorized smart cards, as taught by Perlman et al., with the method of Leppek/Maillard et al./Schneier. It would have been obvious to combine including a database of unauthorized smart cards, as taught by Perlman et al., with the method of Leppek/Maillard et al./Schneier because the provides a listing of all users who are intruders.

Response to Arguments

5. Applicant amends claim 8.

6. Applicant argues:

a. Leppek does not teach a smart card and the combination with Maillard is not obvious (page 16-18).

b. Invention authenticates/authorizes the smart cards instead of securing the message within the smart card (page 19 through page 21).

c. Dependent claims are allowable based on their dependency on independent claims (page 21, last paragraph through end of page 23).

Regarding argument (a), examiner disagrees with applicant. As per the interview on September 1, 2004, examiner portrayed his opinion as to why it would be obvious to combine the Leppek and Maillard reference. The idea was that Leppek taught the concept of not exhausting the entire list of cryptographic keys with one, or even a few, readings. This would prevent an intruder from learning the cryptographic technique used. The idea of combining it with a smart card, from Maillard, is obvious in that technology tends to put once large processing components into smaller and smaller devices.

Regarding argument (b), examiner disagrees with applicant. The combination of Leppek/Maillard/Perlman does teach of authenticating/authorizing the smart card. Leppek teaches a plurality of keys so that an intruder cannot arrive at the encryption method easily. Maillard teaches a smart card. Perlman teaches a database that contains valid/invalid cards. These three references combined teach a smart card that is authorized/authenticated by blacklists that may be obtained from a network periodically.

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand as rejected.

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. However, my new number will be 571-272-3863 after our October 25 move. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoff

BH

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100